Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 20: "The Present and Future of Cyber Insurance, With Yosha DeLong"

Speakers: Kevin Szczepanski, Barclay Damon and Yosha DeLong, Global Head of Cyber, Mosaic Insurance

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of the Cyber Sip. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey, everyone. We're back again with Yosha DeLong, senior vice president and global head of cyber for Mosaic Insurance, a NexGen global specialty lines insurer. Welcome back to Cyber Sip, Yosha.

[Yosha DeLong]: Great. Thanks.

[Kevin]: So in our first episode, we talked about the origins of the cyber market dating back to the late '90s and early aught years of this century. We talked about how you got involved. We talked a little bit about underwriting and how cyber underwriters help organizations improve their cyber hygiene even as they apply for insurance. Today, I want to shift focus, if we can, and talk about the future of cyber coverage and to sort of ask you your thoughts on where the market is heading today. I know you're asked about that all the time, but that's sort of it: the question, like where are we going to be in five years' time?

[Yosha]: Yeah, no. And it's fun to think about because, you know, where are we going to be in six months? Right. Where we are we going to be in three years, where are we going to be in 10 years? There's just so many different directions that the cyber market can take. And we're seeing threats change literally on a daily basis and what's going on with the threat actors changing on a daily basis. So Conti is one of the top ransomware gangs, and there was an announcement that I read yesterday that they're actually somewhat shutting down and splitting up. So what's that going to mean? And what is a fraction, fractioning of a gang mean? Is that going to mean that there's less policing of their people and people are just going to go rogue and go out on their own? Or does it mean that we're going to see some people that are getting out of it now and less bad actors? We don't really know at this point in time. And that could be a something short term that we do see in the next...play out in the next couple of months. When you look at, you know, insurance products and our response to those types of threats, I think we have built an insurance product, you know, which we talked about last time that was really in response to a very particular type of event that was happening in the early 2000s around privacy. And, you know, if you still look at some of the old policies, that's what they are. They're called "privacy forms," you know?

[Kevin]: Right.

[Yosha]: And so when you think of the threats that we have now, we continue to add to these policies to address the threats that have come along and the impact that it's had on businesses in order to properly make

sure that they're...they do have some financial backing to these types of events. But when we look at how they're going to change in the future...is the format we've taken right now, is this continuing, you know, "Frankensteining" of a privacy policy going to be the right way to go? Or do we come to a point where we just scrap everything that we've done in the future and everything that we've done the past and start looking at the future as a completely different product. And I keep thinking that's what's going to happen, especially as we have been over the past couple of years, looking to remove the cyber exposure from, you know, property policies, from casualty policies. And those exclusions continue to get broad mean and there is more demand to have clarification around whether or not you are covering cyber in various policies. There are gaps in coverage right now, and we don't really have great solutions for that. You know, does a policy just become completely bespoke where, you know, I'm talking to some of our national accounts clients and they're saying, well, I don't need this and this. I just want to focus on this, or I just need this, you know? And so, are we completely going to be just manuscripting policies for everyone out there? There's lots of different directions it could go, but I think that's really exciting because that's an opportunity, opportunity for all of us. And, you know, you don't always get that the insurance industry. So.

[Kevin]: No. You really are on the cutting edge. A couple of things you mentioned I wanted to talk to, walk back to. And you were talking about property and some of the I think it was professional lines policies where there is this silent cyber coverage. Can you talk a little bit about that? Because I think on one hand, very creative and excellent policyholder coverage lawyers will do their very best to exploit those gaps and vulnerabilities in a policy for the benefit of their clients. We understand that. I'm, truth be told, I'm on the outside, or the opposite side of that. I'm the one fighting against that. But I respect it. Part of the concern I have with silent cyber is that in one or a few claims, the policyholder may win the battle, but ultimately it's going to lose the war because these gaps are going to be closed. And if the policyholder doesn't have a standalone cyber policy, they may be left bare when something really bad happens. Can you talk a little bit about silent cyber as a risk in the market today?

[Yosha]: Yeah, yeah. I mean, that's something I've been dealing with the past five or six years. I think it's ...there's lots of different ways to take it. And there are some policies that are, you know, what we call silent on cyber that actually intend on covering a cyber event. So, you know, for example, worker's comp, which is highly regulated and the forms are highly regulated. If a hacker hacks into a manufacturing plant and they take over a robotic arm and that robotic arm swings around and, you know, injures somebody, that worker's comp policy is still going to apply because it is there to address, you know, a worker getting injured on the job. There are...there is not the ability to say, okay, we're not going to cover it because a cyberattack actually caused it. So, you know, those types of policies, auto policies which are highly regulated, you know, if somehow a hacker was able to get a hold of someone's car, which cars are moving computers in this day and age and, you know, disable the brakes remotely and it causes an accident, that's still going to be covered under your auto policy. Where there has been a lot of discussion around silent cyber is whether there's areas that we really intend on covering based on kind of antiquated policy wording. So the focus has really been on the property space; a little bit in the casualty space as well. But I would say mostly in the property—you know, what constitutes property, what constitutes physical damage, you know, is damage to data, damage to property? When a server gets fried or somebody's entire manufacturing plant gets fried, should that be covered under a property policy or should that be covered under a cyber policy? So this is really what the industry has been struggling with and there's been a lot of wording have been pushed out, you know, Lloyd's is really good about pushing out wordings that provide some market guidance and saying this is how we should be addressing it. But then it's also leaving gaps of the cyber, the cyber policy, cyber market just isn't quite ready to step up and say, okay, yeah, we're going to cover those property damages when they're not covered at property policy, or we're going to cover that third party, you know, liability when it's not covered under a liability policy. So all of us in the market working together to say this is what we intend on covering. And I do think there are certain aspects that property should cover. But they need to add clarity around their wordings on what

they're covering and what they're not. So the way I always say it, you know, and I've been working on lots of different coverages, lots of different policies for years is we need to make sure that we ring fence it, define it, we're charging appropriately for it. We're explaining it to the brokers, explaining it to our lawyers that are doing coverage work so that they're able to explain it to the clients. Because nobody wants surprises and we don't want policies to end up in litigation, even when, like you said, even when the, you know, insurance, when these things...they've spent, you know, tons and tons of money on these cases. And that's not the direction you want to go in. And you really want to look for clarity and market certainty in the policies.

[Kevin]: Right. So one of the things that has helped the casualty industry, I think, over time is standardized forms. ISO has provided those for decades. And though they have evolved over time, you have a lot of carriers using very similar language. So the market gets used to that and has standard definitions, as you mentioned. Do you see anything like that on the horizon for cyber? I was once in an advising conference and a very knowledgeable and funny gentleman who was speaking in saying, you know, comparing cyber policies to each other is not like comparing apples to oranges. It's more like apples and hand grenades. It's just, they're very different forms. Very difficult for the market to digest and understand. Is there anything coming on the horizon that may make that easier, or do carriers simply prefer to have their own tried and true language?

[Yosha]: Yeah. I mean, what we have seen is that the latter; the carriers prefer to have their own language. But that doesn't mean that we don't, you know, continue to have that conversation. And the common language, the conversation, you know, I've worked with the Geneva Association on it. I've worked with the US Chamber of Commerce, and we've lobbied for some of these things to go through government and say, you know, let's set some standards. And if we take the standards and we can kind of go from there, I think the challenge is the continuous threats. And really, you know, the market itself is so large. And so there's going to be carriers that are very established, carriers that really write like the lower part of the middle market, and the threats that they're going to experience and that maybe the types of claims they're seeing and the remedial actions that need to be taken are going to be very different than maybe, you know, a Carrier B that's over here that's writing in national accounts based on a primary basis. But I do think that there needs to be a focus in the market about simplifying the way we word these and really being very straightforward with how the coverage is going to play out in an event. And when we started Mosaic, I pulled up seven or eight of my top competitor's policy forms. I mean, apples to oranges. We're talking about like, you know, a pineapple and a cherry. I mean, it's like some of them are written to address events and some of them are written to address the outcome of events. You know, I mean, it's not even like the way that that they flow goes the same, you know. So it's very interesting. But they're all, you know, they're all out there in the market and clients have different preferences for that. So, you know, maybe that's going to continue just because that's the way clients like it. And there's different segments that are going to appeal to different segments of clients.

[Kevin]: Right. And frankly, I don't mind that. I don't mind the free approach because it frees up companies like yours to go out and compete on that, the strength of that different language. And you're going to be competing in an ever-hardening marketplace, right. So let's talk for a bit just about what it means that the market is hardening right now. And then I wanted to talk with you a little bit about some of the ways in which coverage is contracting and then maybe some of the ways in which it is expanding at the same time.

[Yosha]: Yeah, really looking at how the market got into the position, you know, we started seeing a shift, I would say, towards the end of 2019. But when...I have this really great visual PowerPoint that that explains this, but I think I can do it just orally. So we saw, you know, 2015 a lot of claims that were coming out of data-breach claims. And last time we spoke, I mentioned, you know, Target and Home

Depot were two of the ones that people were really talking about. We saw a bit of a spike then. We also saw increase in people buying coverage. After that, probably around 2016, we started to see the prices being driven down a bit because people were like, oh, well, this is a really interesting coverage, we want to be in this market. And the loss ratios prior to those events were very, very good. So, you know, people, okay, we can make money. This is a catastrophic coverage. It's only going to happen to these types of companies. It's only going to happen to companies that have credit cards and consumers. So people you know, we went from, I think like 23 carriers to like 200 carriers in the cyberspace in a matter of years. So as you.

[Kevin]: An explosion.

[Yosha]: Yeah, you increase the competition, it's driving down the price. At that same time, we were seeing an increase in threats that was really expanding the coverage. And, you know, the biggest one was really business interruption. So you have an event and your business has to shut down. You know, what revenues have you lost as a result of that? You know, there's a lot of other factors in there, but that's a very basic way to explain it. So that was the expanding coverage and then other things started getting layered on top of that. And as those coverages expanded, there wasn't necessarily a upload in the premium to result from that. So you were kind of expanding the coverages, premiums are coming down. And then we saw the ransomware start to increase and there was a collision really of ...we cannot continue to make money off this. We were looking at these as cap policies. We were looking at these as high severity, low frequency...ransomware completely turned that on its back. And now we're seeing frequency where I was hearing in the market, you know, people were saying, oh, we're seeing 100 claims a month out of ransomware. We're seeing 200 claims a month, where in the past they've been seen maybe five or six cyber incidents a month.

[Kevin]: Wow.

[Yosha]: So the strain on the carriers was huge and the costs were huge and the forensics firm's costs were going up. And, you know, there weren't as many forensics firms in the market at that time as we see now. So it was really a kind of a perfect storm that happened. And the market basically said this is unsustainable; if we don't do something, you know, we're not going to be around in the next five years.

[Kevin]: So what did the market do? Did companies get out of the business? Did they tighten their underwriting requirements? And if so, how did they tighten those underwriting requirements in a way that made the risk more palatable to underwrite?

[Yosha]: Yeah, I think, you know, I would say three big things. We were kind of moving towards asking less and less questions. And I remember going out to brokers and they're like, well, you know, this market only asked three questions. They asked for their name, address, and website and they can underwrite off that. That stopped happening. So, you know, that plays into the way we underwrite, really looking at the controls, what kind of controls they have, how they're going to recover from that, how they're going to prevent an event from happening in the first place. Things that are particular to their industry as well. You know, health care company is very different than a retail company, which can be very different than the manufacturing. And is this manufacturing highly automated versus non–highly automated? They need to have different controls in place, but there's still like a minimum set of controls that everyone should have in place, no matter what kind of information you have, no matter what you do in your industry. So there was a focus on that. The other thing was really the capacity, and we definitely started to see this towards the end of 2020. But you know, when we opened shop in Mosaic, it just happened to be the perfect timing for us because there was such a shift in the market and there was a need for a new player, which was, you know, we just kind of slid right into that by accident. But I'm definitely very happy that it happened.

[Kevin]: Good accident.

[Yosha]: Yeah. So carriers that were offering $25 million in limits all of a sudden said, well, we don't want to have this much exposed to one event, so we're going to constrict that down to tens. And then it was, you know, we said we used to say tens, fifteens are the new tens, you know, oh well now people are only offering fives. And we were getting... as soon as we open our doors, we're getting all these calls from brokers that are just like, we just need you to fill a hole. You know, if you...it's either yes or no, name your price, fill the hole. We need the capacity. So we didn't really see markets leave the industry, but those were the two biggest things. And I would say the third factor was really looking at the companies and how much they were willing to take themselves. So really looking at their SIRs, you know, their deductibles, we saw those go way up, especially in the national accounts space. But I would say even in the S&B space where we started saying, okay, rather than a $500 deductible, or a thousand deductible, well, you need to have a little skin in the game. You need to show us that you're committed to preventing these events. So, you know, you need a $25,000 deductible. You need this to sting a little bit if it happens so that you do everything in your power to make sure it doesn't. And you don't just see insurance or risk transfer as a replacement for actually paying attention to your cybersecurity.

[Kevin]: You know, and as difficult as I'm sure that was for the industry to react and adjust to, I think in the long run that is one of the things that has led the industry, the policcyholder side, to become more focused and more responsible when it comes to cyber hygiene. Cause $25,000 is significant. I mean, that could be I know the IBM and Ponemon have their reports of the costs of the annual cost of a data breach. But really quite a lot of those expenses can fall within that deductible. And if you have put...if you've invested in that ounce of prevention, you're going to save yourself from what...

[Yosha]: Yeah, that's another good point. You know, I was talking to brokers like eight or nine years ago and they were really frustrated that their clients that did invest in their own cybersecurity and did invest in making sure that they were doing everything right, they felt like they weren't really getting credit in the market for that. And they were kind of you know, these brokers were like, well, why is my client going to invest in this if you guys aren't acknowledging that? And now we're acknowledging it and we you know, there is price difference, but it's also you might not be able to even get the coverage if you don't do these minimum things. But then when you are doing the right things and you are committed to preventing these events and you are committed to working with your carriers to make sure that, you know, they're a partner through the process. They're, you know...you get priced accordingly. And that's the way it should be.

[Kevin]: Right. So far, we've talked about some of the ways in which the coverage has financially contracted. And by that, I guess, I mean premiums go up, limits go down. There's more excess layering in the process to achieve what could have been achieved just a few years ago by a single carrier. Talk to us about some of the other limitations or exclusions that you've seen in the coverage over the last one to two years. I know that there is special emphasis these days on what has been called a systemic cyber risk, so that many carriers are taking a much harder look at a loss that may arise from a systemic ransomware operation as opposed to a smaller one-off that may be more palatable from an underwriting standpoint.

[Yosha]: Yeah, and I think that's probably the biggest one. But when we started to see these shifts in the market and the constriction of limits, I personally did expect to see huge shifts in the wordings. And that didn't happen. It was more where we saw some constriction and some people saying, okay, we need to tighten this up or clean up this wording or we need to, you know, one of the big ones was, for a long time, we were looking at the potential of a third-party loss upstream and downstream. So, you know, you have somebody who's providing a service to you and they have an event. And

that affects your business, and your business's ability to operate. Then the insurance policy would apply. And then on the other end of that, you have an event and your supplier can't function and then they sue you and the policy response to that. So, you know, we kept seeing that getting expanded, expanded. And so that was one area that we saw quickly constrict, but it was more about what defined a service provider rather than the coverage just completely going away. So the wording got really broad, like, you know, anyone that you had a material dependency on or something along those lines to either naming, you know, we're going to name these three critical suppliers and then the underwriters can kind of underwrite them to a certain extent, realize where their accumulation could be or, you know, saying like, it's only this type of service provider. So that was one area where we did see—I would say it was more of a clarification, well was a tightening of the wordings. It was really a clarification allowing underwriters to get really their hands around what they were actually covering. But the systemic event has been a huge topic of conversation ever since the WannaCry and NotPetya incidents in 2016 and '17. We realized, like one of these large-scale events could really be detrimental to the insurance industry. And that's detrimental to the insurance industry, the reinsurance industry. And then you're talking.

[Kevin]: You're talking about a global, global risk.

[Yosha]: Yeah. Yeah. And, you know, and reinsurers don't just reinsure cyber, they reinsure other things, too. So that could result in hardening markets across other lines of business as well, just based on the financial stability of these companies. So there's been a lot of conversations around what do we want to cover, what do we not want to cover? How do we continue to make sure that we are sustainable for the future? And every time one of these events happens, SolarWinds event, a Kaseya event, they are large scale, but they're not large scale, on, like where they're going to impact the entire industry. But we start to say, okay, this is what could happen, this is what could happen. How are we going to put controls around this? So there's lots of ways that, you can underwrite to those types of events. And that's really how we're building our portfolio is looking at, you know, diversification across industries. So if I'm not 100% concentrated in a dentist's office, then the dentist's office software that goes down isn't going to completely blow up my portfolio. And so, you know, looking at what companies' dependencies are and making sure that you have diversification across your portfolio. But as far as wordings, the industry has really been looking at how we address that. And there is a market out there that put out a systemic event wordings, and kind of trying to control that. And I think that that's really driving the discussion and whether or not it's the right way to handle it is going to be determined by the applicability of it and the, you know, the longevity that we start to see in the market. But it's moving in the right direction as far as addressing the problem. And then it's really going to say, set the stage for other people to say, you know, do we think that's the right direction or do we want to handle something different, which leads us all the way back to the beginning of our conversation. Or we could have 15 different versions of ways to handle this in the next couple of years.

[Kevin]: Yeah. So you were talking about some of the large scale events that did not have the global impact that perhaps some had expected, or that they might have, in a different context. And I know you've talked recently about the Russia-Ukraine war, and we've we're all aware of the potential cyber risk. I think a lot of people fully appreciate the scale of the cyberattacks that are going back and forth between those two nations right now. Is that an example of one of the events that the industry is concerned about becoming global? Can you talk to us a little bit about that? Because I think the way this was reported in the media, we were all we were expecting there to be a full-on cyber crisis when the war began. That didn't happen. And I feel like we may not be paying careful enough attention to what's really going on, may not be fully prepared for an explosion in this risk.

[Yosha]: Yeah, I think, you know, cyber war, we could do a whole 'nother episode about cyber war. It's a very interesting topic and how the industry is looking at it. We've been doing a lot of work around really

defining what we do want to cover and don't want to cover in that space. And what constitutes cyber war? What cyber war could turn into. But I think, you know, explicitly with the with the Ukraine-Russia situation, it's a horrible thing to watch unfold. And I think the humanitarian crisis that it has caused has just been absolutely gut-wrenching. And knowing that cyber is one of the warfare tools that is being used right now on both sides is really interesting to watch. And we have seen it, you know, it may not have been as well-reported, but there's been there's been some pretty severe incidents on both sides that have tried to take down critical infrastructure, that have tried to really damage the way that people operate and live their daily lives, these types of things. One of the most interesting things that came out of this is that a lot of the bad actors that were working together in these gangs had members in both Ukraine and Russia, and it caused kind of a division of them having to declare their loyalty. And we actually saw some of the major gangs divide up and some fractions caused, which could have actual implications where we saw a bit of a decrease in ransomware elsewhere at the beginning of this. And you know, in talking to the people that are kind of on the front lines with this kind of stuff, you know, they said, well, this could either create an opportunity where we see somebody else like a, you know, Iran or a Iran or a China step in and say, okay, there's a vacuum and we're going to take advantage of that. Or it could be a situation where they're going to be...because Russia spending so much money on this war, they could be more motivated to start to commit ransomware events to help fund the war. We haven't really seen that yet, but there is, in Russia in particular, it's not a highly organized government-run operation, not like what we see out of China or North Korea. So, you know, it's a little bit more of a government-allowed type of thing. And the government can induce them to commit certain crimes and have the financial kickback from that. But I think there's still some stuff to come out. And like you said, you know, I think we're going to be looking back on this probably in a year from now. And there's going to be things that we're not aware of right now that are going on. But then the other huge concern and, you know, we saw this with the not one or with NotPetya was it was Russia attacking Ukraine, but it got out of the country. And so that's what we keep talking about is, you know, we want to make sure that our insureds that have nothing to do with those two, but have some connection to an Ukrainian company if they somehow are impacted by a direct thing, you know, so we call it an indirect attack because they're not the direct target. You know, they should be covered in most cases, you know, subject to policy wording, of course. And this shouldn't be something that we really are looking to exclude unless we have been very explicit in the policy that we want to exclude it. So we're really looking at making sure that there's clarity around that. And there's a lot of projects going on in Lloyd's right now around what war should mean and where we don't want to, as an industry, be covering war exposure.

[Kevin]: No, I think that's critical. And what I'm hearing as you're talking us through this is the risk of a spillover effect. So if you're an Ukrainian company, then you may be doing business with an Ukrainian company. And if this and...as that web expands, you could have businesses in the United States, for example, that have only indirect connections to Ukrainian or Russian businesses, but they will be affected if there is a...an attack on one of those directly affected organizations. So very interesting.

[Yosha]: That goes back to our cyber hygiene. And if they're doing the right cyber hygiene things, then, you know, they have that backstop, right? Patching is a huge part of that patching. You...

[Kevin]: No, critical. And it's amazing that in 2022, we're talking about some of the very same elements of cyber hygiene and we're talking about multi-factor authentication, smart passwords, patching. I tell clients sometimes, you know, if you do three things, if you do those three things, you will be 50 to 80 percent more secure than you are now. But we do still see clients coming to us suffering from attacks, and we say, well, do you have multi-factor authentication? And many are still not in that position, which sort of speaks to the challenge of the industry. Well, before we go, and you've been so kind to spend this time with us today, I want to ask you about some of what I'm calling expansions of coverage. Some of these have been around for a little while, but I want to talk a little bit about the three Bs, I guess, contingent business interruption, which you were talking about earlier when

you were mentioning vendors who may... if I am a food manufacturer and my spice supplier suffers a cyberattack, am I covered for the loss of business? That's sort of a CBI claim. And then I wanted to ask you about bricking and betterment too. Betterment, especially because that's been a gap in coverage over time that is starting to get filled. So, can we start with the CBI and work through those?

[Yosha]: Yeah. And CBI is something that we, we do see as a fairly essential coverage. But I think that again goes back to that clarity around what is covered and what isn't and how we're looking at covering that because CBI is really the greatest source of systemic event. Because if you have a vendor that's a vendor to multiple companies, which most of them are, they usually don't have one client and vulnerability is discovered, that vulnerability can spread to all those different clients. So that's really...while I don't expect CBI coverage to go away any time, I think there's going to be some clarity around what the industry is looking to do. And it also goes back to us as underwriters making sure that we understand what those dependencies are on the contingent business interruption clients. So what are you actually relying on them for? How important is this? And you know, how many clients do we have in our portfolio that have vulnerability to this particular vendor? So somewhat on the underwriters to really start to look at some of those checks and balances on that.

[Kevin]: That can greatly complicate the underwriting process, though. Right. And you alluded to it earlier with sort of the...perhaps limiting the coverage to key vendors, maybe two or three. Otherwise, your underwriter effectively has to underwrite multiple vendors in order to get a real handle on the insured's risk.

[Yosha]: Yeah. Yeah. And, I keep saying, I was in London last week and having some of these conversations. And I always said, I picture it like, you know, the red string where we've got, okay, this client's got this and this client's got this, and then we look at where the intersections are. Of course, I'm simplifying it way more because we actually have AI and computers that do all this stuff for us, and it's part of the modeling process, but it's going to be really important to realize. But I also think the industry is going to have to say, you know, at what point do you draw the line? Like, if I'm...if I have a massive portfolio of primary carriers and like, do I suddenly say, okay, I'm not taking any more carrier that has, you know, a dependency on this particular vendor and then just draw the line like property does and property says, okay, we're full. We have no more room for Florida. We're done. We haven't done that as an industry yet. So it'll be interesting to see how that develops and part of the underwriting process as we start to track some of this information.

[Kevin]: It's an evolving process and it evolves over such a short period of time.

[Yosha]: Bricking was the other one you mentioned, and I think bricking is so interesting because when we were first writing this, these policies, you know, bricking is essentially a piece of hardware getting so fried that it turns into a brick and it's useless and there's no way to really remediate that. And those can be quite costly. But when people used to have server farms on-site and they held a lot of servers, that was our main concern was really, you know, what happens when all those servers get fried and all the data is lost and you've got the data restoration costs as part of the policy and then, you know, but somebody might have millions and millions worth of hardware. That's also where we're starting to see this play out more is in the manufacturing industry and the manufacturing industry, especially this highly automated, using robotics, using things like that. They have a huge dependency on hardware that's not in the traditional form that you would think of, like a server or a computer. But they're very sophisticated machines that can be quite costly, and that's where that really comes into play. And so as an underwriter, if you're offering a coverage like that, you're really looking at what's my exposure to this particular insured? And that kind of determines, is this something you want to offer them? Do you supplement it? Do they really understand? Are they really paying for the coverage and the exposure that's presented? So that's been one that's been interesting to see it evolve because when we were first talking about this maybe six years ago, we're like, well, you know, it's

not really something that...it's actually physical property damage, which is something we're not really looking to cover. So, you know, should that be covered under our property policy and started to have those conversations again.

[Kevin]: Finally betterment, which has always been near and dear to my heart, because when I've had to explain to a client who has suffered a cyber incident that the good news is your forensic service provider, your carrier's provided this vendor to help you. They can go in, they can figure out who got in, where they went, what was exfiltrated or accessed. And they can help you fix the glitch. But, if they discover that your system is deficient in some way, you're responsible for repairing or remediating on your own. Improvements were not covered for the longest time, but that has changed.

[Yosha]: It has changed. We've really seen it as something that's been advantageous to the carriers. So, you know, if somebody breaks into your house and it's because you have a broken lock on your back door, your insurance company pays, you know, they're not going to say, okay, well, good luck, you know, we hope you get that fixed in the next couple of months. It's really to our benefit to say, okay, we're going to either give you a small amount within the policy to pay for this and actually get these computer systems up to a level they need to be so that we can close these back doors and close these vulnerabilities and make sure this doesn't happen again. So it is an advantage to the insurance company to know that that was done and really be able to have some feeling that you can stand this risk because you know that now there is a minimum standard. But I would say that also comes into the underwriting when we start to look at legacy systems and how people are controlling their legacy systems. So do we want to underwrite a company that has a lot of legacy systems or has a lot of outdated software and hardware? So that's part of the underwriting process and saying, you know, okay, there might be something that they have, maybe it's offline, maybe they have it because there's no ... not any other company that can make this particular machine or whatever it is. But I think it really comes into play when we talk about medical devices. And we have yet to see where, you know, medical device causes a huge ransom event. Thankfully...

[Kevin]: Right? Not yet.

[Yosha]: And a lot of how to ringfence those and keep those out of their network. But, you know, that could be something where we say, okay, you know, these things, they need to be there needs to be a more modern MRI machine put in here that can actually be patched versus this this one that you have sitting around here for the last 30 years.

[Kevin]: So it just it sounds like the risks are increasing. And while the market is tightening, the industry is responding by expanding coverage, clarifying coverage in the key areas to enable policyholders to manage and transfer these ever-increasing risks.

[Yosha]: Yeah, that's exactly it. And I think that clarification is a huge, huge part of it. The market, the industry needs to be very clear about what we want to cover and what we don't do, and making sure that the clients understand how to best utilize their policies, partner with their carriers, partner with their brokers, really try to become the best that they can at this, preventing these events and understand the implications of an event throughout their organization. And, you know, those are really going to be key to the longevity of this market.

[Kevin]: Well, I think that's a great place to leave it. So we'll leave it there. Yosha DeLong, thank you so much for joining us. And I really look forward to talking with you again on another episode.

[Yosha]: Great. Thank you so much, Kevin. I really enjoyed this.

[Kevin]: Thanks to you and thanks to all of you for watching this episode of Cyber Sip. We're back soon with another one.

[Kevin]: The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.